Exercise 7

Foundation of Cryptography, Fall 2011

Idan Bachar

February 1, 2012

Let $g : \{0,1\}^n \mapsto \{0,1\}^{3n}$ be a PRG and consider the commitment scheme in the question, we want to show that it is statistically binding and computationally hiding.

We will first prove the following lemma:
Lemma 1: Let $g : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a PRG, $\{R_n\}_{n\in\mathbb{N}}$ an efficiently samplabe ensemble of distributions such that $\forall n \in \mathbb{N} : Supp(R_n) \subseteq \{0,1\}^{l(n)}$, then the ensemble $\{G_n\}_{n\in\mathbb{N}}$, where $G_n = (g(x) \oplus r)_{x\leftarrow\{0,1\}^n, r\leftarrow R_n}$ is computationally indistinguishable from the ensemble $\{U_{l(n)}\}_{n\in\mathbb{N}}$
Proof: Assume by contradiction that the above ensembles are not computationally indistinguishable, then there exists a PPT D, a polynomial p and an infinite $I \subseteq N$ such that for any $n \in I$:
$|\Pr_{x\leftarrow G_n}[D(1^n, x) = 1] - \Pr_{x\leftarrow U_{l(n)}}(D(1^n, x) = 1]| > \frac{1}{p(n)}$ which means
$|\Pr_{r\leftarrow R_n, x\leftarrow g(U_n)}[D(1^n, x \oplus r) = 1] - \Pr_{x\leftarrow U_{l(n)}}(D(1^n, x) = 1]| > \frac{1}{p(n)}$
Define:

Algorithm 1 D'

Input: $1^n, x \in \{0,1\}^{l(n)}$
$r \leftarrow R_n$
return $D(1^n, x \oplus r)$

We claim that D' can distinguish between the output of $g(U_n)$ and $U_{l(n)}$:

$$|\Pr_{x\leftarrow g(U_n)}[D'(1^n, x) = 1] - \Pr_{x\leftarrow U_{l(n)}}[D'(1^n, x) = 1]| =$$
$$|\Pr_{r\leftarrow R_n, x\leftarrow g(U_n)}[D(1^n, x \oplus r) = 1] - \Pr_{r\leftarrow R_n, x\leftarrow U_{l(n)}}[D(1^n, x \oplus r) = 1]| =$$

Because $U_{l(n)} \oplus r \equiv U_{l(n)}$, we get:
$= |\Pr_{r\leftarrow R_n, x\leftarrow g(U_n)}[D(1^n, x \oplus r) = 1] - \Pr_{x\leftarrow U_{l(n)}}[D(1^n, x) = 1]| > \frac{1}{p(n)}$
In contradiction to g being a PRG.

Hiding:
We want to show that for every PPT R^*:
$\{View_{R^*}(S(0), R^*)(1^n)\}_{n\in\mathbf{N}} \approx_c \{View_{R^*}(S(1), R^*)(1^n)\}_{n\in\mathbf{N}}$
Assume by contradiction that there exists a PPT R^* such that the above distributions are not computationally indistinguishable which means there exists a PPT A, a polynomial p and an infinite $I \subseteq N$ such that for every $n \in I$:

$$|\Pr[A(View_{R^*}(S(0), R^*)(1^n)) = 1] - \Pr[A(View_{R^*}(S(1), R^*)(1^n)) = 1]| > \frac{1}{p(n)}$$

We will use R^* and A to distinguish between a $g(U_n)$ and U_{3n} which will in contradiction to g being a PRG.
We note that in our case the view of R^* is 1^n, the value of r it sends to S, $g(U_n)$ for $S(0)$ and $g(U_n) \oplus r$ for $S(1)$.
Define $\{R_n\}_{n\in N}$ to be the distribution ensemble from which R^* selects r.
The above inequality can be written as:
$|\Pr_{r\leftarrow R_n}[A(g(U_n), r, 1^n) = 1] - \Pr_{r\leftarrow R_n}[A(g(U_n) \oplus r, r, 1^n) = 1]| > \frac{1}{p(n)}$
Therefore, using the triangle inequality:

$$\begin{gathered}
|\Pr_{r\leftarrow R_n}[A(g(U_n), r, 1^n) = 1] - \Pr_{r\leftarrow R_n}[A(U_{3n}, r, 1^n) = 1]| + \\
|\Pr_{r\leftarrow R_n}[A(U_{3n}, r, 1^n) = 1] - \Pr_{r\leftarrow R_n}[A(g(U_n) \oplus r, r, 1^n) = 1]| \geq \\
|\Pr_{r\leftarrow R_n}[A(g(U_n), r, 1^n) = 1] - \Pr_{r\leftarrow R_n}[A(U_{3n}, r, 1^n) = 1] + \\
\Pr_{r\leftarrow R_n}[A(U_{3n}, r, 1^n) = 1] - \Pr_{r\leftarrow R_n}[A(g(U_n) \oplus r, r, 1^n) = 1]| > \frac{1}{p(n)}
\end{gathered}$$

We get that at least one of the following must hold for infinitely many n's:
(1) $|\Pr_{r\leftarrow R_n}[A(g(U_n), r, 1^n) = 1] - \Pr_{r\leftarrow R_n}[A(U_{3n}, r, 1^n) = 1]| > \frac{1}{2p(n)}$
(2) $|\Pr_{r\leftarrow R_n}[A(g(U_n) \oplus r, r, 1^n) = 1] - \Pr_{r\leftarrow R_n}[A(U_{3n}, r, 1^n) = 1]| > \frac{1}{2p(n)}$
Now define a PPT D as follows:

Algorithm 2 D

Input:$1^n, x \in \{0, 1\}^{3n}$

- $r \leftarrow R_n$
- return $A(x, r, 1^n)$

If (1) is true, we claim that D can distinguish between the output of $g(U_n)$ and U_{3n} which contradicts g being a PRG:

$$|\Pr[D(1^n, g(U_n)) = 1] - \Pr[D(1^n, U_{3n}) = 1]| =$$
$$|\Pr_{r\leftarrow R_n}[A(g(U_n), r, 1^n) = 1] - \Pr_{r\leftarrow R_n}[A(U_{3n}, r, 1^n) = 1]| > \frac{1}{2p(n)}$$

Assume that (2) is true, construct $\{G_n\}_{n\in\mathbb{N}}, \{U_{3n}\}_{n\in\mathbb{N}}$ as in Lemma 1. Then:

$$|\Pr_{x\in G_n}[D(1^n, x) = 1] - \Pr_{x\in U_{3n}}[D(1^n, x) = 1]| =$$
$$|\Pr_{r\in R_n, x\in U_n}[D(1^n, g(x)\oplus r) = 1] - \Pr_{r\in R_n, x\in U_{3n}}[D(1^n, x) = 1]| > \frac{1}{2p(n)}$$

Hence, $\{G_n\}_{n\in\mathbb{N}}$ and $\{U_{3n}\}_{n\in\mathbb{N}}$ are not computationally indistinguishable, which using Lemma 1 contradicts g being a PRG.

Binding:
We want to show that for any algorithm S^* and security parameter 1^n:

$$\Pr[S^* \text{ interacts with R and outputs a commitment c, } (b, x) \leftarrow S^*,$$
$$(b', x') \leftarrow S^* : b \neq b' \wedge R(b, x, c) = R(b', x', c) = 1] = neg(n)$$

w.l.o.g assume that $b = 0$ and $b' = 1$.
Let $r \in \{0,1\}^{3n}$ be the value R sent to S^* in the commitment stage.
For $R(0, x, c)$ and $R(1, x', c)$ to accept, S^* needs to find $x, x' \in \{0,1\}^n$ such that $c = g(x)$ and $c = g(x') \oplus r \Rightarrow r = g(x) \oplus g(x')$
Hence, for each pair $g(x), g(x')$ there is exactly one such r.
The PRG g is a function from $\{0,1\}^n$ so $|Im(g)| \leq 2^n$ which means there are at most 2^{2n} such pairs ($|\{g(x) \oplus g(x') : x, x' \in \{0,1\}^n\}| \leq 2^{2n}$) and therefore at most 2^{2n} r's for which such pairs exist.
From the claim above and since $r \in \{0,1\}^{3n}$ we get that the probability that such a pair exist for a uniformly selected r is at most $\frac{2^{2n}}{2^{3n}} = \frac{1}{2^n}$, that is $\Pr_{r\in\{0,1\}^{3n}}[\exists x, x' \in \{0,1\}^n : g(x) = g(x') \oplus r] \leq \frac{1}{2^n}$. We get that:

$$\Pr[S^* \text{interacts with R and outputs a commitment c, } (b, x) \leftarrow S^*,$$
$$(b', x') \leftarrow S^* : b \neq b' \wedge R(b, x, c) = R(b', x', c) = 1] \leq \frac{1}{2^n}$$

so the scheme is statistically binding.